Broken Hash Crash? IOTA's Price Keeps Dropping on Tech Critique

Daniel Palmer
Sep 8, 2017 at 16:50 UTC | Updated Sep 9, 2017 at 13:35 UTC

FEATURE

The IOTA-U.S. dollar exchange rate (IOT/USD) has plummeted in the last 24 hours following revelations from Boston University and MIT researchers that cryptographic vulnerabilities had led to a patch in the widely touted cryptocurrency's code.

Heralded for its corporate partnerships and unique technology that enables fee-free micropayments, the project had long attracted grumblings from developers who questioned the strength of its design. Still, market sentiment has been bullish, with IOTA's market capitalization rising to more than $1 billion on its unprecedented debut in June.

While developers involved in the project have pushed back against the claims, and their impact, the high-profile assessment was nonetheless pointed in its critique.

Neha Nerula, director of MIT's Digital Currency Initiative, wrote:

> *"When we noticed that the IOTA developers had written their own hash function, it was a huge red flag. It should probably have been a huge red flag for anyone involved with IOTA."*

The market, it seems, is now in the process of pricing in that critique - and IOTA has certainly taken one on the chin.

The cryptocurrency traded at the daily low of $0.5210 at press time. As per CoinMarketCap, IOTA has lost more than 20 percent in the last 24 hours and, week-on-week, is down 23 percent.

The news of IOTA's broken hash function is certainly bearish in the short run as it means investors will need to come to terms with the reality that the cryptocurrency space is still new and thus vulnerable to such errors.

However, on a monthly basis, it is still up 16 percent, thus the broader trend is still bullish.

The fact that the error was detected and reported by reputable researchers, and the flexibility and speed shown by the IOTA team in fixing the bug, could end up boosting confidence that, in the long run, robust and useful technologies will one day emerge from the sector.

Falling channel breached to the downside

Daily chart

Investopedia defines "falling channel" or "descending channel" as a price action contained between two downward sloping parallel lines: i.e. lower highs and lower lows.

The falling channel has been breached to the downside, in the case of IOTA. An end of the day close below the channel would signal the bears have regained control.

View

- A daily close below the falling channel would open up downside towards $0.3633 (September 4 low) and $0.2365 (July 25 low)
- The 14-day RSI is bearish, suggesting scope for more sell-off of IOTA
- Only a move above $0.7488 (September 6 high) would signal trend reversal from bearish to bullish.

Broken light bulb image via Shutterstock

The leader in blockchain news, CoinDesk is a media outlet that strives for the highest journalistic standards and abides by a strict set of editorial policies. CoinDesk is an independent operating subsidiary of Digital Currency Group, which invests in cryptocurrencies and blockchain startups.

Disclaimer: This article should not be taken as, and is not intended to provide, investment advice. Please conduct your own thorough research before investing in any cryptocurrency.

Prices Security Markets IOTA

PREVIOUS ARTICLE

Metropolis Ahead: Ethereum Developers Set September Date for...

NEXT ARTICLE

Sprint and SsoftBank Back New Blockchain Consortium for...

RELATED STORIES

Mar 9, 2018 at 14:00 | Omkar Godbole
Bitcoin Drops 20% But Wasn't Week's Big Crypto Price Loser

Mar 9, 2018 at 10:00 | Omkar Godbole
Bears in Control, But Bitcoin Eyes $8K Defense

Mar 9, 2018 at 05:20 | Wolfie Zhao
Bitcoin Drops Below $9K As Crypto Falls to 1-Month Low

Mar 8, 2018 at 17:49 | Nikhilesh De
$800 in 1 Hour: Bitcoin Price Drops Big to Near $9K

Comments for this thread are now closed.

56 Comments CoinDesk Login

Recommend Share Sort by Best

Saul Espinosa • 6 months ago

The IOTA team patched this over a month ago when it was brought up to them and they even mention it as one of the reasons we had to transition update to new seeds. This is old news but oddly enough the hit piece article comes out of nowhere over a month after being patched.

Proof this was already fixed and public a month ago. The below quoted article dated August 7th from their blog post update.

"One of the cryptographers we reached out to months ago to review Curl has disclosed that he is worried there might be a potential vulnerability in Curl. We have since had our internal team, as well as other cryptographers review it and asked the disclosing party for more information. While the party that did the responsible disclosure has been quite forthcoming, there are still some of the last details to be discussed more thoroughly with the respective teams in order to reproduce the claims and verify if there was even any vulnerability. However, even though we have protection mechanisms in place that would render even most valid attacks useless in this 'training wheel stage' (due to the Coordinator and the higher-level protocol), as you are working on the cutting edge you have to take every precaution possible and always be on guard. Therefore we have made the simple decision to temporarily switch Curl with Keccak (SHA-3) for cryptographic signing in IOTA."

Very strange to have a sudden hit piece regarding a long since fixed public issue that was hardly open to exploit.

This is also why we have the coordinator for shit like this in the early stages of IOTA. Yet the fudsters would want to tell you we shouldn't and should just remain open to attack this early in IOTAs development lol.

see more

19 • Share ›

Pizza Mampf ➚ Saul Espinosa • 6 months ago

I hate such rookie articles - halfheartedly investigated, problem was fixed immediately by the devs and not the slightest negative thing happens for holders.

7 • Share ›

dr evil ➚ Pizza Mampf • 6 months ago

there actualy wasn't even a "bug" or "problem" .. .. it was all fud to begin with .. but ppl go nuts reading "MIT" in some report and although they did show some problems.. in reality it could never work

2 • Share ›

Enlightened Doggo ➚ Saul Espinosa • 6 months ago

Maybe it was a hit piece. However, this should have never happened in the first place. These guys have no business writing encryption software if they are going to do boneheaded things like write up and deploy a new hash function for no reason.

1 • Share ›

Mark Jones ➚ Enlightened Doggo • 6 months ago

Really? There is a very good reason; they need a function that works with ternary. Please stop repeating talking points without doing a little research first.

2 • Share ›

Enlightened Doggo ➚ Mark Jones • 6 months ago

Sounds like you are the one that needs to do some research, because it was supposed to be a trinary hash function. And no, that is not a good reason to ship an experimental hash function into production code. Real quantum computers don't even exist yet, so they could have clearly been more cautious. They weren't even experts on the algorithm that they were forking. Expect to hear of more exploits in the future if their security practices continue being this incoherent.

1 • Share ›

Mark Jones ➚ Enlightened Doggo • 6 months ago

Please go and read up on the matter before circulating even more FUD. The hash function wasn't even being used in anything critical to the project. I don't care if you like IOTA or not, but repeating story points when you have obviously haven't done the research is not very intelligent. If you want to have the last word, go for it, but you're wrong and nothing's going to change that.

• Share ›

Enlightened Doggo ➚ Mark Jones • 6 months ago

to a metric butt ton of other peoples production machines without proper vetting _first_ lol.

Share ›

Per Lind ➚ Mark Jones • 6 months ago

Zactly2!

Share ›

Per Lind ➚ Saul Espinosa • 6 months ago

Zactly!

Share ›

Rizwan Khan • 6 months ago

excerpt from Neha's article: """ We informed the IOTA developers, they patched their system, and we wrote a vulnerability report. The current version of IOTA does not have the vulnerabilities we found """"

10 Share ›

JO89 • 6 months ago

The author of this article has no market background and was formally an employee of igot.com (which ended up bankrupt)..... very reputable.... smh

14 Share ›

Crypto Cunnie • 6 months ago

Keep fudding...the response from the IOTA team:
https://blog.iota.org/curl-...

8 Share ›

zer0n1ght • 6 months ago

Crap article. IOTA is still feeling the effects of the China ICO Ban announcement. It reached even lower than .5 long before this misleading "vulnerability" critique was made. On that subject, the critique was highly uninformed. They found an attack vector, but unless you are magical it would be impossible to actually carry out the attack do to the nature of the DAG / Tangle. So it wasn't really a major threat at any point, and has already been resolved. I think people are just trying to attack the next best thing to protect their investments in other inferior coins at this point. How about you google the numerous vulnerabilities found in Bitcoin while you are at it.

6 Share ›

no whammy ➚ zer0n1ght • 6 months ago

They do. Bitcoin takes more incoming than anyone. Why the cheap shot?

Share ›

FlowMotions • 6 months ago

Clickbait!
You don't even recognize that the broken hash function is not used for any critical parts.

Also: https://gist.githubusercont...

9 Share ›

J Mark • 6 months ago

The problem was theoretical, almost impossible to exploit in practice. It was fixed and no funds were in danger. It was a while back. Why is this published on 08 sept I don't know.

3 Share ›

Tragic Mishap • 6 months ago

Right so when Iota goes from 15 cents to a dollar CoinDesk says absolutely nothing. This is literally the first time I've seen Iota in a headline here and it's bogus FUD. This ain't suspicious or anything.

3 Share ›

Nikato Muirhead • 6 months ago

This article speaks of the exploit in the present-Tense, that has already been patched. Forces invested in the bitcoin blockchain are trying to Donald Trump a fine cryptocurrency. Very sad and shameful.

5 Share ›

Marcio Romano • 6 months ago

The vulnerabilities have already been fixed! Why are you trying to denigrate or to discredit un amazing and revolutionary project? This kind of journalism with negative intent are made only by dishonest people.

2 Share ›

JO89 • 6 months ago

... shhh....Straight FUD. Do your research. This was already fixed a month ago.

Share ›

Mark Jones • 6 months ago

It's amazing that nobody's questions why a person involved with Z-Cash didn't disclose that fact when making a overly critical disclosure of something their competitor fixed a month prior and, in any case, did not have ANY real world chance of causing a loss of IOTA even if it hadn't been.

1 ^ | v • Share ›

Patrick Little • 6 months ago

The big news is the is the exposure of ternary and the so-called Trusted Private Coordinator they would have to fork out later to be permission-less and the whopper, they wrote their own Hash?? They were begging for a review. These are real doubts. If investors were not getting answers, I don't blame them for MIT involvement. IOTA, welcome to public review. Now, let's see that coordinator code...

2 ^ | v • Share ›

Sean ➚ Patrick Little • 6 months ago

They WERE begging for a review... Literally... As in IOTA's development team asked MIT to review the code, not any investors etc as you claim.

1 ^ | v • Share ›

Patrick Little ➚ Sean • 6 months ago

My response is currently detected as SPAM and a modified response is under review.

^ | v • Share ›

Patrick Little ➚ Sean • 6 months ago

I have had such reviews and they do request your permission to publish well before some principles have already looked through a request and they would give a prospectus of focus. It takes someone to pay for the resources. In one case, principles showed up unannounced to an organized bake-off, requested access to the device, ran their tests and only after not being able to bring the device to its knees, revealed their test case. I found out later third party review was requested by the event sponsor. It's fine to have strong opinion, but please ask around in informed circles. Suggestion by experience not a claim. I am always happy to be proved wrong. Writing and implementing one's own hash functions from scratch is what begged for review by third party, logical. Third Party review and publication will only strengthen IOTA's products if they want wide acceptance. It is a very natural progression in engineering. I had to take out the referenced third party actual names as even here it was detected as SPAM, really? Public Opinion Censorship, really???

^ | v • Share ›

Mark Jones ➚ Patrick Little • 6 months ago

Sure, there are real doubts but as of yet, nobody has found a flaw in the code. The involvement by MIT was REQUESTED BY THE IOTA TEAM for crying out loud. Dom has published ALL of his interactions with the team and the Medium article was just a hit piece.

1 ^ | v • Share ›

Patrick Little ➚ Mark Jones • 6 months ago

I have read the IOTA whitepaper and I would target the hash as well as the ternary use, plus a few more items. The coordinator was not detailed. I would be happy to read it if it was published on their site. Engineering should be welcoming to review. Publicity, good or bad, will result in more welcoming avenues. Resiliency to challenges is always a plus. To truly succeed, the keys always have to be turned over and MIT is one that is trusted.

^ | v • Share ›

Mark Jones ➚ Patrick Little • 6 months ago

How do you trust a team that did not disclose their conflicts of interest (involvements in other cryptocurrencies) and instead of publishing under the MIT banner, used Medium to publish a misleading article that had a heading that can, at minimum, be deemed click-bait and at another extreme be considered libelous.

^ | v • Share ›

Patrick Little ➚ Mark Jones • 6 months ago

Most likely, because I have been tested. IF you have been you'd find them worthy.

^ | v • Share ›

mltbg • 6 months ago

yep, that IOTA is just another fools gold

3 ^ | v • Share ›

Harley Quinn • 6 months ago

IOTA is a scam

1 ^ | v • Share ›

Share ›

Pizza Mampf ➚ Harley Quinn • 6 months ago
crybaby-noob :p
1 Share ›

Marcio Romano ➚ Harley Quinn • 6 months ago
As your mother
1 Share ›

Harley Quinn ➚ Marcio Romano • 6 months ago
You don't even have a mother, your fag father pull you out of his ass.
Share ›

Per Lind • 6 months ago
And where is IOTA today! Very poor scaremongering!
Share ›

kelechi • 6 months ago
this is a definitive rejoinder.....https://medium.com/@mistywind/iota-...
Share ›

Luey Forje • 6 months ago
The truth is here, it was not even a vulnerability in the first place, its there by design to prevent clones. https://gist.githubusercont...
Share ›

Ciristian Martinez • 6 months ago
ai21btc predicts the value of bitcoin in the short term,the successes in the predictions are amazing and it's free.
Share ›

J Mark ➚ Ciristian Martinez • 6 months ago
I'm sure you would spread the word about a bot that could make you millions if it's any good. #not.
Share ›

Camaman • 6 months ago
When was this known? weeks ago?
Not sure if 10% of the drop was due to this already fixed bug that most investors dont understand.
Rest of the drop being on fake news from china, al criptos blindly following Bitcoin trend and the fact that it is friday....

I personaly got stuck with it due to Bitfinex having Limit order as default instead of Market.
That was a -25% lesson on double checking your balance currency before lunch...
Share ›

dr evil ➚ Camaman • 6 months ago
buy and hold man.. it's going +1$ some day .. maybe next weeks
Share ›

Camaman ➚ dr evil • 6 months ago
Lol!
Probably will.
Buy and hold is most likely better tecnique than trading for these things.
Unless you do it for monthly income
1 Share ›

danystatic • 6 months ago
I simply can not see it recovering , there are so many alternatives for people to invest in. Yeah, sure David Sonstab0 has a cool name, but recovery on IOTA is not happening, not any time soon, not weeks, maybe even months, and many other projects are coming, increasing the distribution of money. But again, I might be wrong.
Share ›

JO89 ➚ danystatic • 6 months ago
lol i think you might be wrong. Iota up 22% right now.
Share ›

danystatic ➚ JO89 • 6 months ago
Lol, it's such a crazy market. Let's see in a few weeks

ıths ago

Well good think that they had a centralized back bone, so no problem they can not fix, /sarcasm

Share ›

Adam ➚ Erik • 6 months ago

It's only centralized for the time being so they can continue working on development. I would rather sacrifice temporary centralization in exchange for something that can scale exponentially and have zero fees.

1 Share ›

Erik ➚ Adam • 6 months ago

That's what you hope, for my experience, the lack of redundancy will be a fatal flaw in time, and the creators of this coin now this very well, but in the mean time it does not mean the can pick up a fat paycheck.

Share ›

Load more comments

Bitcoin	$9,290.75
Ethereum	$730.12
Bitcoin Cash	$1,053.1
Litecoin	$188.15
XRP	$0.8372

What category of decentralized applications are you most interested in?

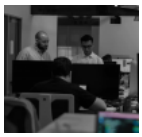
- Prediction markets
- Storage
- Token exchange

VOTE

Features

Progress Slows On Once-Hot Ethereum Privacy Projects

Sierra Leone Secretly Holds First Blockchain-Powered Presidential Vote



Compliant ICOs? Bitcoin OGs Launch Token Sale Service

Comcast Makes First Big Bet on a Multi-Blockchain Future

Have a breaking story?

Let us know here »